UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,503	09/02/2003	Len L. Mizrah	AIDT 1005-1	3753

22470 7590 05/01/2008
HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
05/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/653,503	MIZRAH, LEN L.	
	Examiner	Art Unit	
	Farid Homayounmehr	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4,6,7,9-11,13,14,16-18,20,21 and 31-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 9/30/2003; amendment filed 2/11/2008.

2. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39 have been considered. Claims 1, 5, 8, 12, 15, 19, 22-30 cancelled by the applicant. Claims 31-39 are new.

Response to Arguments

3. Applicant has cancelled the claims subject to rejection under section 112. The associated rejection is hereby withdrawn. See the new grounds of rejection in the next section. Applicant's argument relative to rejection under section 103 is moot in view of the new ground of rejection outlined in the following sections.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 37-39 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in

the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Said claims include the term "machine readable data storage medium", which is not described or defined in the Specification. It is not clear what encompasses "machine readable data storage medium".

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman, (US patent 6363480, March 26, 2002), in view of Kelly (US Patent No. 5,636,280, dated June 3,1997), and further in view of Official Notice.

6.1 As per claim 31, Perlman is directed to a method for mutual authentication in communications between first and second stations, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key

initiation intervals (fig. 1 and the associated text, particularly col. 5 lines 10-25);

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key (col. 6 lines 1-20);

sending a message carrying said associated session key to the second station (col. 6 lines 17-20),

and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (Perlman col. 6 lines 21- 35 teaches receiving a message from the second party, encrypted with the communicated session key (note that Perlman col 2 lines 20-35 suggests using short term keys (ephemeral) in setting up a session key. The SSL protocol certifies and authenticates the keys established to secure the communication session). However, Perlman does not specifically teach a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the

second station and to identify the second station or the user of the second station. Kelly teaches authentication of parties of communication to each other and verification of session key based on a shared secret. Kelly col. 7 lines 5-50 specifically teach after the session key is established, in item (d) of the authentication protocol, a password (shared secret) is encrypted using the session key and sent to the host. The host verifies the password, and authenticates the other party.

Perlman and Kelly are analogous art as they are both directed to key distribution and user authentication in security systems based on cryptographic processes.

At the time of invention, it would have been obvious to the person skilled in art to combine the method of secured key exchange as taught by Kelly with the method of ephemeral key distribution as taught by Perlman. Kelly teaches a method to securely deliver keys from one party to another. Perlman teaches use of multiple ephemeral keys to secure the communication session, which requires transmission of ephemeral keys from one party to the other. Therefore, the one skilled in art would be motivated to use the method of Kelly to deliver the ephemeral keys of Perlman from one party to the other.);

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation

interval (this limitation creates n ephemeral keys, with the same characteristics of Perlman's ephemeral keys discussed above. An iterative process, which repeats the same steps, and how it is taught in the prior art is discussed in the following);

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users (the verification of the digital identifier at the first party is discussed in Kelly col. 7 lines 5-50),

the first set of exchanges including sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges, receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i) (this process repeats the steps discussed in the first exchange

of messages, by using the key verified in the first iteration in the second iteration (key (i) and Key (i-1)).

In other words, the above process is an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations discussed above. Namely, during the first to the (n-1)th iteration, the system repeats sending a new key, encrypted from one station to the other. The new key is encrypted with a key known to both parties (the previous session key). The receiving side decrypts the encrypted new key and uses it as the new session key Column 5, lines 55 - Column 6, lines 20. Perlman's teaching of ephemeral keys is for the purpose substituting a key with another after the lifetime of a key is expired. Therefore, the session keys are substituted with a fresh key after expiration of their lifetime. This whole process is discussed in the above. In the nth and (n+1)th iteration, the same process continues, with the exception that in the nth iteration the shared secret is used to encrypt the new key, and in the (n+1)th iteration a second shared secret is use for the same. This technique is also discussed above. The nth and (n+1)th iterations also includes creating a hash of the session key, which the Examiner takes the Official Notice to be also a well-known technique in the art. Therefore, all steps of the iterative method are discussed, and shown as prior art in the above. Also, using an iterative technique to improve the security of the cryptographic protocol is well known in the art. Reference is made to the DES protocol, which basically deploys a plurality of stages that scrambles the input data iteratively, and each iterative stage uses a different

parameter (a key) to perform a different operation. The key in each stage is extracted from the previous stage. As another example, reference is made to "Applied Cryptography" by B. Schneier, page 53 (a copy is attached to this Office Action). Section titled SKEY, clearly teaches the concept of repeated application of a cryptographic technique to improve the security of the protocol. Therefore, given enough resources and time, it would have been obvious to use an iterative method, which includes a known process at each iterative stage to improve the security of the protocol.);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,
receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and
decrypting the hashed version of the intermediate data key (n), calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;
sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and
if the second station sends a response to the second message, carrying a hashed

version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations (the second set of exchanges again involves an iteration process, similar to what is discussed above, with a difference of using a second shared secret in addition to the first shared secret, and using a hashed version of an encryption key to encrypt the key. However, using the second shared secret is again repeating the same process where the first secret was used. Also use of a hashed version of a key is known in the art, as exemplified in DES protocol.); and if mutual authentication is verified at the first station, then sending a message indicating successful authentication (Kelly Col. 6 lines 57-62).

6.2. As per claim 32, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of 3 said intermediate data keys (i) (encryption using a key such as key(n-1) was well known in the art at the time of invention. The motivation to do so would be to secure the message by delivering it in cipher text rather than clear text.

6.3. As per claim 33, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session (The purpose of establishing keys between parties of communication is encrypting the message for the purpose of confidentiality protection, or integrity protection).

6.4. As per claim 2, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including using said associated session key in response to another request to initiate a communication session from a third station received by the first station for first exchanges in the during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval (Perlman in view of Kelly, further in view of Official Notice teaches use of a associated session key in response to a request to initiate a communication session from any station received by the first

station for first exchanges in the during said particular session key initiation interval. Therefore, the combination teaches use of an associated session key in response to another request to initiate a communication session from a third station received by the first station for first exchanges in the during said particular session key initiation interval (see response to claim 31). The combination also teaches use of another set of ephemeral keys after one is expired).

6.5. As per claim 3, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 3, including associating a unique set of intermediate data keys with each session key (the combination discloses the method of claim 2, including assigning said session random key to all communication sessions initiated with the first station during said session random key initiation interval, and associating a different set of ephemeral intermediate data random keys with each communication session, where the first party announces a set of ephemeral key pairs (Column 5, lines 55-67) and each time the second party desires to launch a communication session with the first party, a key is selected from the list (and therefore is unique), and the first party passes the key to the second party (Column 6, lines 1-20)).

6.6. As per claim 4, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including:
providing a buffer at the first station (Perlman Column 6, lines 35-57); storing the set of ephemeral session keys in the buffer (Column 5, lines 55- 67 & Column 6, lines 35-57.

Note that the session keys are ephemeral keys and are stored only during their lifetime) and removing session keys from said buffer upon expiry of respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals (the ephemeral keys are removed from buffer when expired, as shown in claim 31. Per column 6, lines 35-67, the lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that it is usable after the set up period is completed is a obvious, logical and trivial choice. It is a trivial choice to choose the lifetime of session keys to be longer than the initiation intervals because the initiation interval is part of the session).

6.7. As per claim 6, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges for the plurality of exchanges used to distribute the symmetric in expected circumstances (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that they last long enough for completion of verification is a logical and obvious choice).

6.8. As per claim 7, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 4, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual

authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10 (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that the key is usable after any multiple of time it takes to complete the set up period is a logical and obvious choice).

6.9. Requirements of claims 9-11, 13-18, 20 and 21 are substantially the same as claims 31-33, 3, 4, 5-7 discussed above.

6.10. Requirements of claims 34-36, and 37-39 are substantially the same as claims 31-33 discussed above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139